EXHIBIT A

SUPREME COURT FOR THE STATE OF NEW YORK
NEW YORK COUNTY

ILISE HEITZNER, individually and on behalf of all others similarly situated, Plaintiff, -v- NORTHWELL HEALTH, INC. and PERRY JOHNSON & ASSOCIATES, INC., Defendants.	Index No.: **SUMMONS**

TO THE ABOVE NAMED DEFENDANTS:

YOU ARE HEREBY SUMMONED to answer the Class Action Complaint (the "Complaint") in this action and to serve a copy of your answer or, if the Complaint is not served with this summons, to serve a notice of appearance on plaintiff's attorneys within twenty (20) days after service of this summons, exclusive of the day of service; or within thirty (30) days after completion of service if the service is made in any manner other than by personal delivery within the state; or if service of the summons is made by mail pursuant to CPLR §312-a, you must complete and mail or deliver the acknowledgement of receipt to the undersigned within thirty (30) days from date of receipt and serve an answer within twenty (20) days after the signed acknowledgement is mailed or delivered to the undersigned, and in case of your failure to appear or answer, judgment will be taken against you by default for the relief demanded in the Complaint.

Plaintiff designates New York County as the place of trial. The basis of venue is the place of business of one or more of the defendants.

Dated: New York, New York
November 15, 2023

Respectfully submitted,

NEWMAN FERRARA LLP

/s/ Jeffrey M. Norton

Jeffrey M. Norton
Benjamin D. Baker
1250 Broadway, 27th floor
New York, NY 10001
Tel. (212) 619-5400
jnorton@nfllp.com
bbaker@nfllp.com

SUPREME COURT FOR THE STATE OF NEW YORK
NEW YORK COUNTY

ILISE HEITZNER, individually and on behalf of all others similarly situated, Plaintiff, -v- NORTHWELL HEALTH, INC. and PERRY JOHNSON & ASSOCIATES, INC., Defendants.	Index No.: **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Ilise Heitzner ("Plaintiff") brings this class action against defendants Northwell Health, Inc. ("Northwell") and Perry Johnson & Associates, Inc. ("PJ&A," and together with Northwell, "Defendants"), and alleges as follows upon personal knowledge as to Plaintiff and Plaintiff's own acts and experiences, and, as to all other matters, upon information and belief, including investigation conducted by Plaintiff's attorneys.

NATURE OF THE ACTION

1. Plaintiff brings this class action against Defendants for their failure to properly secure and safeguard personally identifiable and financial information ("PII") and protected health information ("PHI") of Plaintiff and the Class members, including, without limitation: names, dates of birth, home addresses, medical record numbers, hospital account numbers, and clinical information such as the names of the treatment facility, the names of healthcare providers, admission diagnosis, and date(s) and time(s) of service.

2. Defendants are a nonprofit integrated healthcare network that is New York State's largest healthcare provider and a provider of certain transcription and dictation services.

3. Defendants are entrusted with an extensive amount of the Plaintiff's and the Class members' PII and PHI.

4. By obtaining, collecting, using, and delivering a benefit from Plaintiff's and Class members' PII and PHI, Defendants assumed legal and equitable duties to Plaintiff and the Class members.

5. On or around March 27, 2023 to May 2, 2023, an intruder gained unauthorized access to PJ&A's systems, accessed Plaintiff's and the Class members' PII and PHI, and exfiltrated information from PJ&A's systems. Then, on or around April 7, 2023 to April 19, 2023, an intruder gained unauthorized access to Northwell's systems, accessed Plaintiff's and the Class members' PII and PHI, and exfiltrated information from Northwell's systems (together, the "Data Breach Incidents").

6. The full extent of the types of sensitive personal information, the scope of the breaches, and the root cause of the Data Breach Incidents is all within the exclusive control of Defendants and their agents, counsel, and forensic security vendors at this phase of litigation.

7. Defendants did not notify Plaintiff and the Class members of the Data Breach Incidents until November 3, 2023.

8. Plaintiff's and the Class members' PII and PHI that was acquired through the Data Breach Incidents can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII and PHI to criminals. Plaintiff and the Class members face a lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers.

9. Plaintiff's and the Class members' PII and PHI was compromised due to Defendants' negligent acts and omissions and the failure to protect Plaintiff's and the Class members' PII and PHI.

10. Plaintiff and Class members continue to be at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

11. Defendants disregarded the rights of Plaintiff and the Class members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure their PII and PHI was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the PII and PHI of Plaintiff and Class members was compromised through access to and exfiltration by at least one unknown and unauthorized third party.

12. Plaintiff bring this action on behalf of all persons whose PII and PHI was compromised because of Defendants' failure to: (i) adequately protect their PII and PHI; (ii) warn of Defendants' inadequate information security practices; and (iii) effectively secure equipment and the database containing protected PII and PHI using reasonable and effective security procedures free of vulnerabilities and incidents.

13. Defendants' conduct amounts to negligence and violates federal and state statutes.

14. Plaintiff and Class members have suffered actual and imminent injuries as a direct result of the Data Breach Incidents, including: (i) theft of their PII and PHI; (ii) costs associated with the detection and prevention of identity theft; (iii) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the consequences of the Data Breach Incidents; (iv) invasion of privacy; (v) the emotional distress and anguish, stress, and annoyance of responding to, and resulting from, the Data Breach Incidents; (vi) the actual and/or imminent injury arising from actual and/or potential fraud and identity theft

posed by their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (vii) damages to and diminution in value of their personal data entrusted to Defendants with the mutual understanding that Defendants would safeguard Plaintiff's and Class members' PII and PHI against theft and not allow access and misuse of their personal data by others; and (viii) the continued risk to their PII and PHI, which remains in the possession of Defendants, and which is subject to further breaches, so long as Defendants fails to undertake appropriate and adequate measures to protect Plaintiff's and Class members' PII and PHI, and, at the very least, are entitled to nominal damages.

15. Plaintiff and Class members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

PARTIES

16. Plaintiff Ilise Heitzner is, and at all times relevant hereto was, a citizen and resident of Westchester County, New York.

17. Defendant Northwell is, and at all times relevant hereto was, a New York corporation with its principal place of business in Nassau County, New York.

18. Defendant PJ&A is, and at all times relevant hereto was, a foreign corporation with its principal place of business in Troy, Michigan.

FACTS

19. At the time of the Data Breach Incidents, Defendants maintained Plaintiff's and the Class members' PII and PHI in their systems.

20. By obtaining, collecting, and storing Plaintiff's and Class members' PII and PHI, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiff's and Class Members' PII and PHI from disclosure.

21. Plaintiff and Class members relied on Defendants to keep their PII and PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

22. Defendants had a duty to adopt reasonable measures to protect Plaintiff's and Class members' PII and PHI from involuntary disclosure to third parties.

23. Prior to the Data Breach Incidents, Defendants should have: (i) encrypted or tokenized the sensitive PII and PHI of Plaintiff and the Class members; (ii) deleted such PII and PHI that they no longer had reason to maintain; (iii) eliminated the potential accessibility of the PII and PHI from the internet and its website where such accessibility was not justified; and (iv) otherwise reviewed and improved the security of its network system that contained the PII and PHI.

24. Prior to the Data Breach Incidents, on information and belief, Defendants did not: (i) encrypt or tokenize the sensitive PII and PHI of Plaintiff and the Class members; (ii) delete such PII and PHI that they no longer had reason to maintain; (iii) eliminate the potential accessibility of the PII and PHI from the internet and its website where such accessibility was not justified; and (iv) otherwise review and improve the security of their network systems that contained the PII and PHI.

25. On or around March 27, 2023 to May 2, 2023, an intruder gained unauthorized access to PJ&A's systems, accessed Plaintiff's and the Class members' PII and PHI, and exfiltrated information from PJ&A's systems.

26. On or around April 7, 2023 to April 19, 2023, an intruder gained unauthorized access to Northwell's systems, accessed Plaintiff's and the Class members' PII and PHI, and exfiltrated information from Northwell's systems.

27. On or about November 3, 2023, Defendants mailed Plaintiff and the Class members a form notice attempting to minimize the Data Breach Event, while admitting that sensitive PII and PHI had been compromised and stolen.

28. Contrary to the self-serving narrative in Defendants' form notice, Plaintiff's and Class members' unencrypted information may end up for sale on the dark web and/or fall into the hands of companies that will use the detailed PII and PHI for targeted marketing without their approval.

29. Defendants failed to use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiff and the Class members.

30. Plaintiff and the Class members have taken reasonable steps to maintain the confidentiality of their PII and PHI, relied on Defendants to keep their PII and PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

31. Defendants could have prevented the Data Breach Incidents by properly securing and encrypting Plaintiff's and Class members' PII and PHI, or Defendants could have destroyed the data, especially old data from former inquiries and/or customers that Defendants had no legal right or responsibility to retain.

32. Defendants' negligence in safeguarding Plaintiff's and the Class members' PII and PHI is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data, especially in the financial sector.

33. Despite the prevalence of public announcements and knowledge of data breach and data security compromises, Defendants failed to take appropriate steps to protect the PII and PHI of Plaintiff and the Class members from being compromised.

34. The ramifications of Defendants' failure to keep secure Plaintiff's and the Class members' PII and PHI are long-lasting and severe. Once PII and PHI is stolen, fraudulent use of that information and damage to victims may continue for years.

35. The PII and PHI of Plaintiff and the Class members was stolen to engage in identity theft and/or to sell it to criminals who will purchase the PII and PHI for that purpose.

36. Moreover, there may be a time lag between when harm occurs versus when it is discovered, and also between when PII and PHI is stolen and when it is used.

37. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding Plaintiff's and the Class members' PII and PHI, and of the foreseeable consequences that would occur if Defendants' data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and the Class members as a result of a breach.

38. Plaintiff and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights.

39. Plaintiff and Class members are incurring and will continue to incur such damages in addition to any fraudulent use of their PII and PHI.

40. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants' networks, potentially amounting to millions of individuals' detailed and confidential personal information and thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

41. The injuries to Plaintiff and the Class members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the Plaintiff's and the Class members' PII and PHI.

42. Plaintiff has suffered and will continue to suffer a substantial risk of imminent identity, financial, and health fraud and theft; emotional anguish and distress resulting from the Data Breach Incidents, including emotional stress and damages about the years of identity fraud Plaintiff faces; and increased time spent reviewing financial statements and credit reports to determine whether there has been fraudulent activity on any of their accounts.

43. Plaintiff has a continuing interest in ensuring that her PII and PHI, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

CLASS ALLEGATIONS

Proposed Class

44. Plaintiff brings this lawsuit as a class action on behalf of herself individually and on behalf of all other similarly situated persons as a class action pursuant to Article 9 of the CPLR.

45. The "Class" that Plaintiff seeks to represent is defined as:

> **All persons whose PII and/or PHI was accessed and/or exfiltrated during the Data Breach Incidents.**

46. Defendants and their employees or agents are excluded from the Class.

Numerosity

47. The Data Breach Incidents have affected as many as 3.9 million people.

48. The members of the Class, therefore, are believed to be so numerous that joinder of all members is impracticable.

49. Identification of the Class members is a matter capable of ministerial determination from Defendants' records.

Common Questions of Law and Fact

50. There are numerous questions of law and fact common to the Class which predominate over any questions affecting only individual members of the Class.

51. Among the questions of law and fact common to the Class are: (i) whether and to what extent Defendants had a duty to protect the PII and PHI Plaintiff and Class members; (ii) whether Defendants failed to adequately safeguard the PII and PHI of Plaintiff and Class members; (iii) when Defendants actually learned of the Data Breach Incidents; (iv) whether Defendants adequately, promptly, and accurately informed Plaintiff and Class members that their PII and PHI had been compromised; (v) whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach Incidents; (vi) whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach Incidents to occur; (vii) whether Plaintiff and the Class members are entitled to actual, consequential, and/or nominal damages as a result of Defendants' wrongful conduct; (viii) whether Plaintiff and the Class members are entitled to restitution as a result of Defendants' wrongful conduct; and (ix) whether Plaintiff and Class members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach Incidents.

52. The common questions in this case are capable of having common answers. Plaintiff and the Class members will have identical claims capable of being efficiently adjudicated and administered in this case.

Typicality

53. Plaintiff's claims are typical of the claims of the Class members, as they are all based on the same factual and legal theories.

Protecting the Interests of the Class Members

54. Plaintiff is a representative who will fully and adequately assert and protect the interests of the Class and have retained competent counsel. Accordingly, Plaintiff is an adequate representative and will fairly and adequately protect the interests of the Class.

Superiority

55. A class action is superior to all other available methods for the fair and efficient adjudication of this lawsuit because individual litigation of the claims of all members of the Class is economically unfeasible and procedurally impracticable.

56. While the aggregate damages sustained by the Class are in the millions of dollars, the individual damages incurred by each member of the Class resulting from Defendants' wrongful conduct are too small to warrant the expense of individual lawsuits.

57. The likelihood of individual Class members prosecuting their own separate claims is remote, and, even if every member of the Class could afford individual litigation, the court system would be unduly burdened by individual litigation of such cases.

58. The prosecution of separate actions by members of the Class would create a risk of establishing inconsistent rulings and/or incompatible standards of conduct for Defendants. For

example, one court might enjoin Defendants from performing the challenged acts, whereas another may not.

59. Additionally, individual actions may be dispositive of the interests of the Class, although certain class members are not parties to such actions.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

60. Plaintiff incorporates paragraphs 1-59 above as if fully set forth herein.

61. Plaintiff brings this claim on behalf of herself and the Class.

62. Defendants collected, stored, used, and benefited from the non-public PII and PHI of Plaintiff and Class members in the procurement and provision of medical services.

63. Defendants had full knowledge of the sensitivity of the PII and PHI and the types of harm that Plaintiff and Class members could and would suffer if the PII and PHI were wrongfully disclosed.

64. By collecting, storing, and using Plaintiff's and Class members' PII and PHI, Defendants owed a duty to Plaintiff and Class members to exercise reasonable care in obtaining, securing, deleting, protecting, and safeguarding the sensitive PII and PHI.

65. Defendants owed a duty to prevent the PII and PHI it received from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

66. Defendants were required to prevent foreseeable harm to Plaintiff and Class members, and therefore had a duty to take adequate and reasonable steps to safeguard their sensitive PII and PHI from unauthorized release or theft.

67. This duty included: (i) designing, maintaining, and testing its data security systems, data storage architecture, and data security protocols to ensure Plaintiff's and Class members' PII and PHI in its possession was adequately secured and protected; (ii) implementing processes that

would detect an unauthorized breach of its security systems and data storage architecture in a timely and adequate manner; (iii) timely acting on all warnings and alerts, including public information, regarding its security vulnerabilities and potential compromise of the PII and PHI of Plaintiff and Class members; and (iv) maintaining data security measurers consistent with industry standards and applicable federal and state laws and other requirements.

68. Defendants had a common law duty to prevent foreseeable harm to Plaintiff and Class members. The duty existed because Plaintiff and Class members were the foreseeable and probable victims of any inadequate security practices of Defendants in its collection, storage, and use of PII and PHI from Plaintiff and Class members.

69. In fact, not only was it foreseeable that Plaintiff and Class members would be harmed by the failure to protect their PII and PHI because malicious actors routinely attempt to steal such information for use in nefarious purposes, but Defendants also knew that it was more likely than not Plaintiff and Class members would be harmed as a result.

70. Defendants' duties to use adequate and reasonable security measures also arose as a result of the special relationship that existed between them, on the one hand, and Plaintiff and Class members, on the other hand. This special relationship arose because Defendants collected, stored, and used the PII and PHI of Plaintiff and Class members for the procurement and provision of health services for Plaintiff and Class members.

71. Defendants alone could have ensured that their security systems and data storage architecture were sufficient to prevent or minimize the Data Breach Incidents.

72. Additionally, the policy of preventing future harm weighs in favor of finding a special relationship between Defendants and Plaintiff and Class members. If companies are not held accountable for failing to take adequate and reasonable security measures to protect the

sensitive PII and PHI in their possession, they will not take the steps that are necessary to protect against future security breaches.

73. The injuries suffered by Plaintiff and Class members were proximately and directly caused by Defendants' failure to follow reasonable, industry standard security measures to protect Plaintiff's and Class members' PII and PHI.

74. When individuals have their personal information stolen, they are at substantial risk for imminent identity theft, and need to take steps to protect themselves, including, for example, utilizing credit monitoring services and purchasing or obtaining credit reports to protect themselves from identity theft.

75. If Defendants had implemented the requisite, industry standard security measures and exercised adequate and reasonable care, data thieves would not have been able to take the PII and PHI of Plaintiff and Class members.

76. Defendants breached these duties through the conduct alleged herein by, including without limitation: (i) failing to protect the PII and PHI in its possession; (ii) failing to maintain adequate computer systems and allowing unauthorized access to and exfiltration of Plaintiff's and Class members' PII and PHI; (iii) failing to disclose the material fact that Defendants' computer systems and data security practices were inadequate to safeguard the PII and PHI in its possession from theft; and (iv) failing to disclose in a timely and accurate manner to Plaintiff and Class members the material fact of the Data Breach Incidents.

77. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiff and Class members, their PII and PHI would not have been compromised.

78. As a direct and proximate result of Defendants' failure to exercise adequate and reasonable care and use commercially adequate and reasonable security measures, the PII and PHI

of Plaintiff and Class members were accessed by ill-intentioned individuals who could and will use the information to commit identity or financial fraud.

79. Plaintiff and Class members face the imminent, certainly impending, and substantially heightened risk of identity theft, fraud, and further misuse of their personal data.

80. There is a temporal and close causal connection between Defendants' failure to implement security measures to protect the PII and PHI of current and former patients and the harm suffered, or risk of imminent harm suffered, by Plaintiff and Class Members.

81. It was foreseeable that Defendants' failure to exercise reasonable care to safeguard the PII and PHI in its possession or control would lead to one or more types of injury to Plaintiff and Class members, and the Data Breach Incidents were foreseeable given the known, high frequency of cyberattacks and data breaches in the healthcare industry.

82. Plaintiff and Class members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew of or should have known of the inherent risks in collecting and storing PII and PHI, the critical importance of providing adequate security of PII and PHI, the current cyber scams being perpetrated on PII and PHI, and that they had inadequate protocols, including security protocols in place to secure the PII and PHI of Plaintiff and Class Members.

83. Defendants' own conduct created the foreseeable risk of harm to Plaintiff and Class members. Defendants' misconduct included their failure to take the steps and opportunities to prevent the Data Breach Incidents and their failure to comply with industry standards for the safekeeping and encrypted authorized disclosure of the PII and PHI of Plaintiff and Class members.

84. Plaintiff and Class members have no ability to protect their PII and PHI that was and is in Defendants' possession. Defendants alone were and are in a position to protect against the harm suffered by Plaintiff and Class members as a result of the Data Breach Incidents.

85. As a direct and proximate result of Defendants' negligence as alleged above, Plaintiff and Class members have suffered, will suffer, or are at increased risk of suffering: (i) the compromise, publication, theft and/or unauthorized use of their PII and PHI; (ii) unauthorized use and misuse of their PII and PHI; (iii) the loss of the opportunity to control how their PII and PHI are used; (iv) out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud; (v) lost opportunity costs and lost wages and time associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach Incidents, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud; (vi) the imminent and certain impending injury flowing from potential fraud and identity theft posed by their PII and PHI being placed in the hands of criminals; (vii) the continued risk to their PII and PHI that is subject to further breaches so long as Defendants fail to undertake appropriate measures to protect the PII and PHI in Defendants' possession; (viii) current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach Incident for the remainder of the lives of Plaintiff and Class members; (ix) loss of privacy; and (x) emotional distress and anguish related to the years of potential identity theft they face.

86. As a direct and proximate result of Defendants' negligence, Plaintiff and Class members have suffered, and continue to suffer, damages arising from the Data Breach Incidents

as described herein and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class, prays for the following relief:

a) an Order certifying this case as a class action on behalf of the Class as defined above, and appointing Plaintiff as the representative of the Class and Plaintiff's counsel as Class Counsel;

b) equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and the Class members' PII and PHI, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and the Class members;

c) injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class members, including but not limited to an Order: (i) requiring Defendants to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws; (ii) requiring Defendants to delete, destroy, and purge the PII and PHI of Plaintiff and Class members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class members; (iii) requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiff' and Class member's PII; (iv) prohibiting Defendants from maintaining

Plaintiff's and Class members' PII on a cloud-based database; (v) requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors; (vi) requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring; (vii) requiring Defendants to audit, test, and train its security personnel regarding any new or modified procedures; (viii) requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems; (ix) requiring Defendants to conduct regular database scanning and securing checks; (x) requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class members; (xi) requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; (xii) requiring Defendants to implement systems of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendants' policies, programs, and systems for protecting

personal identifying information; (xiii) requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated; (xiv) requiring Defendants to meaningfully educate all Class members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves; (xv) requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and (xvi) for a period of 10 years, appointing a qualified and independent third-party assessor to conduct attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

d) for an award of damages, including actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

e) for an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

f) for prejudgment interest on all amounts awarded; and

g) such other and further relief as this Court may deem just and proper.

JURY DEMAND

Plaintiff, individually and on behalf of the Class, hereby demands a trial by jury.

Dated: New York, New York
November 15, 2023

Respectfully submitted,

NEWMAN FERRARA LLP

/s/ Jeffrey M. Norton

Jeffrey M. Norton
Benjamin D. Baker
1250 Broadway, 27th Floor
New York, New York 10001
(212) 619-5400
jnorton@nfllp.com
bbaker@nfllp.com

Attorneys for Plaintiff and Proposed Class

SUPREME COURT OF THE STATE OF NEW YORK
NEW YORK COUNTY

ILISE HEITZNER, individually and on behalf of all others similarly situated,

Plaintiff,

-v-

NORTHWELL HEALTH, INC. and PERRY JOHNSON & ASSOCIATES, INC.,

Defendants.

Index No. 161199/2023

STIPULATION EXTENDING TIME TO ANSWER THE COMPLAINT

WHEREAS, on November 15, 2023, Plaintiff Ilise Heitzner ("Plaintiff"), on behalf of herself and all others similarly situated, filed a Summons and Complaint initiating the above-captioned action (the "Complaint");

WHEREAS, Defendant Northwell Health, Inc.'s ("Northwell") deadline to respond to the Complaint is December 18, 2023;

WHEREAS, on November 28, 2023, counsel for Plaintiff and Defendant met and conferred and agreed to modify Northwell's deadline to respond to the Complaint;

NOW, THEREFORE, IT IS HEREBY STIPULATED AND AGREED by and between the parties hereto through their undersigned counsel that the time for Defendant to respond to the Complaint in this action is hereby extended to and including January 29, 2024.

/ / /

Dated: December 5, 2023

By: */s/ Andrew B. Cashmore*

William L. Roberts
(*pro hac vice* forthcoming)
Kathryn E. Caldwell
(*pro hac vice* forthcoming)
Andrew B. Cashmore
ROPES & GRAY LLP
Prudential Tower
800 Boylston Street
Boston, Massachusetts 02199-3600
Phone: (617) 951-7000
Fax: (617) 951-7050
william.roberts@ropesgray.com
kathryn.caldwell@ropesgray.com
andrew.cashmore@ropesgray.com

Glen J. Dalakian II
(*pro hac vice* forthcoming)
ROPES & GRAY LLP
1211 Avenue of the Americas
New York, New York 10036-8704
Phone: (212) 596-9000
Fax: (212) 596-9090
glen.dalakian@ropesgray.com

Counsel for Defendant Northwell Health, Inc.

By: */s/ Benjamin D. Baker*

Benjamin D. Baker
NEWMAN FERRARA LLP
1250 Broadway, 27th Floor
New York, New York 10001
(212) 619-5400
bbaker@nfllp.com

Counsel for Plaintiff and the Putative Class